

Basic Nuclear Reactor Safety

All energy forms have upsides and downsides. Nuclear energy is no exception. Nuclear energy's upside is the enormous amount of energy produced by uranium-235 fission – about 1.5 million times more energy per gram of fuel than for hydrocarbon fuels. The downside is energy from the decay of radioactive **fission products** continues to produce heat in the reactor fuel even after the fission reaction is terminated. Fission products have half-lives ranging from seconds to millions of years. At reactor shutdown, the power generated by fission product radioactive decay is about 7.5% of reactor operating power. While decay heat generation drops off as shorter **half-life** radioisotopes disappear, one week after reactor shutdown decay heat power is still about 1.5% of reactor operating power. This radioactive **decay heat** must be removed from the reactor fuel to prevent overheating, fuel melting, and release of radioactive material.

Nuclear Power Plant Safety Objectives

There are three operational safety objectives associated with ensuring the integrity of the nuclear reactor fuel and of the multiple radioactive fission product retention barriers – reactor core **reactivity control** (i.e., neutron population control), reactor core **heat removal** capability, and **fission product containment**. These safety objectives are accomplished by means of a three-level defense-in-depth approach. Level 1 is focused on **prevention**, which seeks to avoid completely those operational occurrences that could result in system damage, loss of fuel performance, and abnormal releases of radioactive material. The goal of Level 2 is **protection**, which seeks to terminate unlikely, low-probability incidents and operational occurrences that cause reactor shutdown and could lead to minor fuel damage and small releases of radioactivity. The emphasis of Level 3 is **mitigation**, which seeks to limit the consequences of accidents if they occur despite the intervention of prevention and protection measures.

Prevention measures include reactor design features that provide inherently stable operating characteristics and safety margins, operational instrumentation and automatic controls, plant personnel training, operating procedures, risk-informed maintenance, and periodic component/system testing and inspections.

Protection measures include automatic reactor shutdown, automatic monitoring and safety-system initiation, and guidelines and procedures for managing operational upset conditions.

Mitigation measures include emergency reactor core cooling and heat removal systems, emergency electrical power systems, radioactivity containment barriers/structures, emergency operating procedures, and an

emergency plan to control and minimize the consequences of potential accidents.

Normal Operational Safety

Normal plant operational safety is accomplished by means of defense-in-depth Level 1 (prevention) measures that maintain reactor core reactivity control, provide decay heat removal capability, and assure fission product retention barrier integrity.

Reactivity Control

Reactor reactivity control (i.e., neutron population control) is assured by reactor design features that provide negative feedback for positive reactivity changes in the reactor core. This control is independent of reactor operator action and operates on very short time scales to ensure a controllable rate of change for reactor power level increases.

A redundant Reactor Protection System that can be manually actuated by a reactor operator or automatically actuated by numerous reactor trip signals ensures that neutron-absorbing control rods can be inserted quickly into the reactor core to terminate the reactor core fission chain reaction.

Decay Heat Removal

Following reactor shutdown, the decay heat load continues to decrease as the shorter half-life radioisotopes decay away. However, the longer half-life radioisotopes continue to generate heat for many years. A nuclear power plant shutdown heat removal system consists of redundant pumps to circulate cooling water to remove heat from the reactor core, and redundant heat exchangers that transfer the heat to a plant component cooling water system.

Even after used fuel is removed from the reactor it needs to be placed in a tank of circulating water to remove decay heat for a few years until the generated heat load has been sufficiently reduced such that air cooling is adequate to keep the fuel rods from overheating.

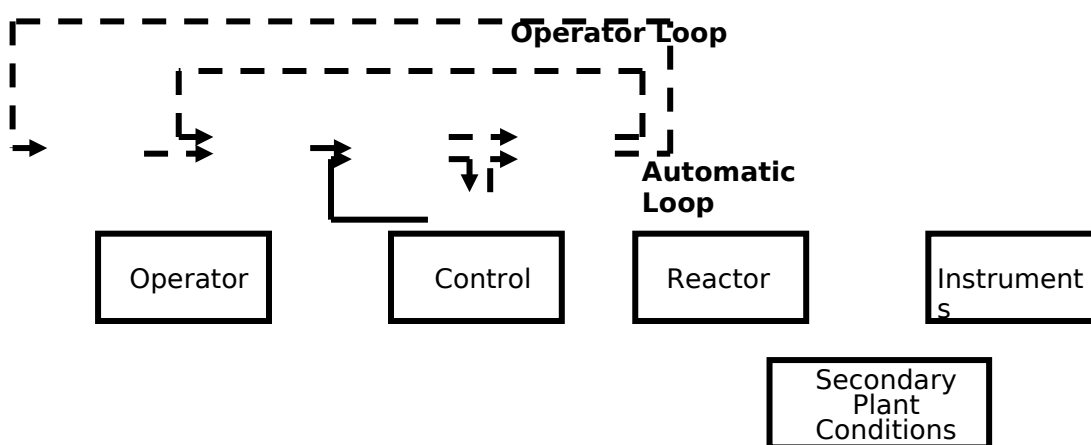
Fission Product Retention Barriers

There are four fission product retention barriers. The first barrier is the uranium oxide fuel pellet. Most fission products are retained within the fuel pellet ceramic matrix. The second barrier is the fuel rod that contains the nuclear fuel pellets. All fission products are retained within the fuel rods as long as they remain intact. The third barrier is the reactor primary coolant system piping and components, which provide a physical barrier to fission product release in the event of fuel rod damage. The final barrier is the reactor containment building structure. This is the ultimate barrier to preventing fission product release to the environment in the event of nuclear fuel damage.

Operational Upset/Accident Safety

In addition to normal operational safety objectives, nuclear power plants have similar safety objectives for operational upset conditions and potential accident events. Plant safety for these situations is accomplished by means of defense-in-depth Level 2 (protection) and Level 3 (mitigation) measures that 1) maintain reactor core reactivity control, 2) provide reactor coolant inventory control, 3) provide reactor core heat removal capability, 4) provide reactor containment building heat removal capability, and 5) assure radioactivity containment.

For normal plant operations, reactor operators are afforded Level 1 reactor control capabilities based on information provided by plant monitoring instrumentation via an operator information loop. For circumstances where operator manual actions may be inadequate, appropriate Level 2 actions are automatically initiated via an automatic information and control loop. This reactor instrumentation and control system is illustrated by the graphic below.



Reactor Core Reactivity Control

The redundant Reactor Protection System (RPS) ensures the reactor core fission chain reaction is terminated for all off-normal operating conditions and events by rapid automatic insertion of control rods into the reactor core. Numerous off-normal plant conditions provide inputs to automatically actuate the RPS.

Reactor Coolant Inventory Control and Core Heat Removal

Emergency Core Cooling Systems (ECCS) are redundant and independent safety systems that provide reactor coolant system makeup water and reactor heat removal in the event of a loss of coolant accident. Both high-pressure and low-pressure injection systems are available to provide makeup water to the reactor coolant system as the system pressure decreases. Low-

pressure injection pumps ultimately recirculate water accumulated from a loss of coolant event and heat is removed from the recirculated water via the plant's decay heat removal system heat exchangers.

Reactor Containment Structure Heat Removal

The Post-Accident Heat Removal System removes heat from the reactor containment structure to prevent over-pressurization following a loss of coolant accident, thereby assuring containment structure integrity. Pumps recirculate accumulated water to containment spray headers and heat is removed from the recirculated water via the plant's decay heat removal system heat exchangers.

Radioactivity Containment

Gaseous and liquid radioactive waste processing systems ensure that all gaseous and liquid effluents from the reactor containment structure are treated to remove radioactive material prior to release so that all post-accident discharges are below regulatory limits.

Engineered Safety System Reliability

The reliability of nuclear power plant engineered safety features is assured by incorporating the principles of redundancy, diversity, and physical separation into their design. Emergency safety systems, including emergency electrical power systems, are completely redundant. Diversity of emergency equipment precludes loss of emergency functions due to common-mode component and system failures. Physical separation of redundant safety systems and equipment, including control and instrumentation electrical cables, assures protection from localized events such as fire and flooding.

The fail-safe principle is also incorporated into the design of plant components. This principle assures that when critical components fail, they fail in a safe condition so they don't complicate an operational upset condition.

Generation 2 versus Generation 3+ Safety System Designs

There is a fundamental safety system design difference between currently operating Generation 2 nuclear power plants and the new Generation 3+ power plants. Generation 2 plants depend on *active* safety measures; for example, AC and DC electrical power for equipment, and early operator intervention for operational upset events. Generation 3+ plants are designed with *passive* safety measures – for example, making use of gravity, natural circulation cooling, and high temperature-resistant materials – and require no operator intervention to manage or terminate operational upsets.

